

This listing of claims replaces all prior versions, and listings of claims in the instant application:

Listing of Claims:

1. (Currently Amended) A method for digital content access control, comprising:

receiving, by a content provisioner, a digital content request from a user device, said digital content request comprising a request for digital content;

creating, by said content provisioner, an authenticated digital content request if a user associated with said digital content request is authorized to access said digital content;

determining, by said content provisioner, one or more delivery parameters, said one or more delivery parameters identifying a target device to receive said digital content; and

sending, by said content provisioner, said authenticated digital content request including said one or more delivery parameters.

2. (Original) The method of claim 1 wherein

said digital content request comprises a Universal Resource Locator (URL);

said authenticated digital content request comprises a tokenized URL; and

said creating further comprises:

determining a token pool associated with said digital content;

determining a token in said token pool; and

creating a tokenized URL based at least in part on said token.

3. (Original) The method of claim 2 wherein said tokenized URL further comprises a cryptogram based at least

in part on an identifier that describes the location of said digital content.

4. (Original) The method of claim 2 wherein said token is from a token pool associated with the location of digital content for which access is authorized.

5. (Currently Amended) The method of claim 1, further comprising synchronizing said content provisioner with said content repository if synchronization is enabled.

6. (Original) The method of claim 1 wherein said one or more delivery parameters comprises a serial number uniquely identifying said target device.

7. (Original) The method of claim 1 wherein said one or more delivery parameters comprises a master key indicator for use in decrypting an encrypted form of said digital content.

8. (Original) The method of claim 1 wherein said one or more delivery parameters comprises a key derivation process indicator for use in deriving a cryptographic key for decrypting an encrypted form of said digital content.

9. (Original) The method of claim 1 wherein said one or more delivery parameters comprises a cryptographic process indicator that specifies a cryptographic process supported by said target device.

10. (Currently Amended) A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for digital content access control, the method comprising:

receiving, by a content provisioner, a digital content request from a user device, said digital

content request comprising a request for digital content;

creating, by said content provisioner, an authenticated digital content request if a user associated with said digital content request is authorized to access said digital content;

determining, by said content provisioner, one or more delivery parameters, said one or more delivery parameters identifying a target device to receive said digital content; and

sending, by said content provisioner, said authenticated digital content request including said one or more delivery parameters.

11. (Original) The program storage device of claim 10 wherein

said digital content request comprises a Universal Resource Locator (URL);

said authenticated digital content request comprises a tokenized URL; and

said creating further comprises:

determining a token pool associated with said digital content;

determining a token in said token pool; and

creating a tokenized URL based at least in part on said token.

12. (Original) The program storage device of claim 11 wherein said tokenized URL further comprises a cryptogram based at least in part on an identifier that describes the location of said digital content.

13. (Original) The program storage device of claim 11 wherein said token is from a token pool associated with the location of digital content for which access is authorized.

14. (Currently Amended) The program storage device of claim 10 wherein said method further comprises synchronizing said content provisioner with ~~saida~~ content repository if synchronization is enabled.

15. (Original) The program storage device of claim 10 wherein said one or more delivery parameters comprises a serial number uniquely identifying said target device.

16. (Original) The program storage device of claim 10 wherein said one or more delivery parameters comprises a master key indicator for use in decrypting an encrypted form of said digital content.

17. (Original) The program storage device of claim 10 wherein said one or more delivery parameters comprises a key derivation process indicator for use in deriving a cryptographic key for decrypting an encrypted form of said digital content.

18. (Original) The program storage device of claim 10 wherein said one or more delivery parameters comprises a cryptographic process indicator that specifies a cryptographic process supported by said target device.

19. (Currently Amended) An apparatus for digital content access control, comprising:

means for receiving, by a content provisioner, a digital content request from a user device, said digital content request comprising a request for digital content;

means for creating, by said content provisioner, an authenticated digital content request if a user associated with said digital content request is authorized to access said digital content;

means for determining, by said content provisioner, one or more delivery parameters, said one

or more delivery parameters identifying a target device to receive said digital content; and

means for sending, by said content provisioner, said authenticated digital content request including said one or more delivery parameters.

20. (Original) The apparatus of claim 19 wherein said digital content request comprises a Universal Resource Locator (URL);

said authenticated digital content request comprises a tokenized URL; and

said means for creating further comprises:

means for determining a token pool associated with said digital content;

means for determining a token in said token pool; and

means for creating a tokenized URL based at least in part on said token.

21. (Original) The apparatus of claim 20 wherein said tokenized URL further comprises a cryptogram based at least in part on an identifier that describes the location of said digital content.

22. (Original) The apparatus of claim 20 wherein said token is from a token pool associated with the location of digital content for which access is authorized.

23. (Currently Amended) The apparatus of claim 19, further comprising means for synchronizing said content provisioner with said content repository if synchronization is enabled.

24. (Original) The apparatus of claim 19 wherein said one or more delivery parameters comprises a serial number uniquely identifying said target device.

25. (Original) The apparatus of claim 19 wherein said one or more delivery parameters comprises a master key indicator for use in decrypting an encrypted form of said digital content.

26. (Original) The apparatus of claim 19 wherein said one or more delivery parameters comprises a key derivation process indicator for use in deriving a cryptographic key for decrypting an encrypted form of said digital content.

27. (Original) The apparatus of claim 19 wherein said one or more delivery parameters comprises a cryptographic process indicator that specifies a cryptographic process supported by said target device.

28. (Currently Amended) An apparatus for digital content access control, the apparatus comprising:

- a memory for storing provisioning information for use in creating an authenticated digital content request that is based at least in part on a digital content request comprising a request for digital content; and

- a content provisioner configured to:

- receive a digital content request from a user device, said digital content request comprising a request for digital content;

- create an authenticated digital content request if a user associated with said digital content request is authorized to access said digital content;

- determine one or more delivery parameters, said one or more delivery parameters identifying a target device to receive said digital content; and

- send said authenticated digital content request including said one or more delivery parameters.

29. (Currently Amended) The apparatus of claim 28 wherein said apparatus is further configured to synchronize with saida content repository if synchronization is enabled.

30. (Currently Amended) The apparatus of claim 28 wherein

said digital content request comprises a Universal Resource Locator (URL);

said authenticated digital content request comprises a tokenized URL; and

said content provisioner is further configured to:
determine a token pool associated with said digital content;

determine a token in said token pool; and

create a tokenized URL based at least in part on said token.

31. (Original) The apparatus of claim 30 wherein said tokenized URL further comprises a cryptogram based at least in part on an identifier that describes the location of said digital content.

32. (Original) The apparatus of claim 30 wherein said token is from a token pool associated with the location of digital content for which access is authorized.

33. (Currently Amended) A method for digital content access control, comprising:

receiving, by a content repository, an authenticated digital content request, including one or more delivery parameters, from a user device, said authenticated digital content request based at least in part on a digital content request comprising a request for digital content wherein said authenticated digital content request was generated by a content provisioner in response to said digital content request from said user device;

validating, by said content repository, said authenticated digital content request, said validating comprising indicating said authenticated digital content request is valid if said authenticated digital content request is validly associated with said digital content and if said authenticated digital content request authenticates said digital content request;

determining, by said content repository, a session key if said authenticated digital content request is valid, said determining comprising:

determining a target key based at least in part on a target ID, said target ID identifying a target device; and

applying a cryptographic process to a first key based at least in part on at least part of said authenticated digital content request together with said target key to create said session key;

encrypting, by said content repository, said digital content using said session key; and

sending, by said content repository, said encrypted digital content.

34. (Original) The method of claim 33 wherein said determining said target key comprises:

determining a master key; and

applying a cryptographic process to said target ID together with said master key to create said target key.

35. (Original) The method of claim 34 wherein said determining said master key is based at least in part on said one or more delivery parameters.

36. (Currently Amended) The method of claim 33, further comprising synchronizing said content repository

with asaid content provisioner if said synchronizing is enabled.

37. (Original) The method of claim 33 wherein
said digital content request comprises a Universal
Resource Locator (URL); and
said authenticated digital content request
comprises a tokenized URL.

38. (Original) The method of claim 33 wherein
said tokenized URL further comprises a token
comprising a cryptogram based at least in part on an
identifier that describes the location of said digital
content; and
said at least part of said authenticated digital
content request comprises said token.

39. (Original) The method of claim 38 wherein said
first key comprises a token key based at least in part on
said token.

40. (Original) The method of claim 38 wherein said
token is from a token pool associated with the location of
digital content for which access is authorized.

41. (Original) The method of claim 33 wherein said
validating further comprises:
receiving a token;
indicating said token is invalid if said token is
not found within a token pool associated with said
digital content or if said token has been fully
redeemed, said token being fully redeemed if the number
of token redemptions equals a predetermined amount; and
incrementing a token redemption count associated
with said token and indicating said token is valid if
said token is found within said token pool and said
token has not been fully redeemed.

42. (Original) The method of claim 33 wherein said validating further comprises:

receiving a token;

indicating said token is invalid if said token is not associated with an partially redeemed or unredeemed offset within a token offset window, said token offset window comprising one or more offset entries identified by a base number and an offset from said base number, said one or more offset entries associated with a token in a token pool formed by applying a cryptographic process to the sum of said base number and said offset from said base number, together with a token chain key, said token pool associated with said digital content; and

updating the offset entry associated with said token and indicating said received token is valid if said token is associated with a partially redeemed offset or unredeemed offset within said token offset window.

43. (Original) The method of claim 33 wherein said validating further comprises:

receiving a token;

indicating said token is invalid if said token is not found within a token pool associated with said digital content or if said token has been redeemed, said token pool formed from successive applications of a cryptographic one-way function;

indicating said token is valid if said token is found within said token pool and said token has not been redeemed; and

invalidating tokens in said token chain that were generated after said received token.

44. (Original) The method of claim 33 wherein said validating further comprises:

receiving a token;

indicating said token is invalid if said token is not found within a portion of a token pool comprising unredeemed tokens, said token pool formed from successive applications of a cryptographic one-way function;

indicating said token is valid if said token is found within said token pool and said token has not been redeemed; and

reordering tokens in said token pool after said indicating said token is valid, said reordering based at least in part on whether the tokens have been redeemed.

45. (Original) The method of claim 33 wherein said validating further comprises:

receiving a token;

initializing a current token to said received token;

applying a cryptographic one-way function to said current token to create a result;

assigning said result to said current token;

repeating said applying until said current token matches a last redeemed token or until all tokens in said pool generated after said received token have been examined;

indicating said token is valid if said current token matches said last redeemed token; and

indicating said token is invalid if said current token does not match said last redeemed token and if all tokens in said pool generated after said received token have been examined.

46. (Original) The method of claim 33 wherein said one or more delivery parameters comprises a serial number uniquely identifying said target device.

47. (Original) The method of claim 33 wherein said one or more delivery parameters comprises a master key indicator for use in decrypting an encrypted form of said digital content.

48. (Original) The method of claim 33 wherein said one or more delivery parameters comprises a key derivation process indicator for use in deriving a cryptographic key for decrypting an encrypted form of said digital content.

49. (Original) The method of claim 33 wherein said one or more delivery parameters comprises a cryptographic process indicator that specifies a cryptographic process supported by said target device.

50. (Currently Amended) A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for digital content access control, the method comprising:

receiving, by a content repository, an authenticated digital content request, including one or more delivery parameters, from a user device, said authenticated digital content request based at least in part on a digital content request comprising a request for digital content wherein said authenticated digital content request was generated by a content provisioner in response to said digital content request from said user device;

validating, by said content repository, said authenticated digital content request, said validating comprising indicating said authenticated digital content request is valid if said authenticated digital content request is validly associated with said digital content and if said authenticated digital content request authenticates said digital content request;

determining, by said content repository, a session key if said authenticated digital content request is valid, said determining comprising:

determining a target key based at least in part on a target ID, said target ID identifying a target device; and

applying a cryptographic process to a first key based at least in part on at least part of said authenticated digital content request together with said target key to create said session key;

encrypting, by said content repository, said digital content using said session key; and

sending, by said content repository, said encrypted digital contentsending said encrypted digital content.

51. (Original) The program storage device of claim 50 wherein said determining said target key comprises:

determining a master key; and

applying a cryptographic process to said target ID together with said master key to create said target key.

52. (Original) The program storage device of claim 51 wherein said determining said master key is based at least in part on said one or more delivery parameters.

53. (Currently Amended) The program storage device of claim 50 wherein said method further comprises synchronizing said content repository with a content provisioner if said synchronizing is enabled.

54. (Original) The program storage device of claim 50 wherein

said digital content request comprises a Universal Resource Locator (URL); and

said authenticated digital content request
comprises a tokenized URL.

55. (Original) The program storage device of claim 54
wherein

said tokenized URL further comprises a token
comprising a cryptogram based at least in part on an
identifier that describes the location of said digital
content; and

said at least part of said authenticated digital
content request comprises said token.

56. (Original) The program storage device of claim 55
wherein said first key comprises a token key based at least
in part on said token.

57. (Original) The program storage device of claim 55
wherein said token is from a token pool associated with the
location of digital content for which access is authorized.

58. (Original) The program storage device of claim 50
wherein said validating further comprises:

receiving a token;

indicating said token is invalid if said token is
not found within a token pool associated with said
digital content or if said token has been fully
redeemed, said token being fully redeemed if the number
of token redemptions equals a predetermined amount; and

incrementing a token redemption count associated
with said token and indicating said token is valid if
said token is found within said token pool and said
token has not been fully redeemed.

59. (Currently Amended) The program storage device of
claim ~~40~~50 wherein said validating further comprises:

receiving a token;

indicating said token is invalid if said token is not associated with an partially redeemed or unredeemed offset within a token offset window, said token offset window comprising one or more offset entries identified by a base number and an offset from said base number, said one or more offset entries associated with a token in a token pool formed by applying a cryptographic process to the sum of said base number and said offset from said base number, together with a token chain key, said token pool associated with said digital content; and

updating the offset entry associated with said token and indicating said received token is valid if said token is associated with a partially redeemed offset or unredeemed offset within said token offset window.

60. (Original) The program storage device of claim 50 wherein said validating further comprises:

receiving a token;

indicating said token is invalid if said token is not found within a token pool associated with said digital content or if said token has been redeemed, said token pool formed from successive applications of a cryptographic one-way function;

indicating said token is valid if said token is found within said token pool and said token has not been redeemed; and

invalidating tokens in said token chain that were generated after said received token.

61. (Original) The program storage device of claim 50 wherein said validating further comprises:

receiving a token;

indicating said token is invalid if said token is not found within a portion of a token pool comprising unredeemed tokens, said token pool formed from

successive applications of a cryptographic one-way function;

indicating said token is valid if said token is found within said token pool and said token has not been redeemed; and

reordering tokens in said token pool after said indicating said token is valid, said reordering based at least in part on whether the tokens have been redeemed.

62. (Original) The program storage device of claim 50 wherein said validating further comprises:

receiving a token;

initializing a current token to said received token;

applying a cryptographic one-way function to said current token to create a result;

assigning said result to said current token;

repeating said applying until said current token matches a last redeemed token or until all tokens in said pool generated after said received token have been examined;

indicating said token is valid if said current token matches said last redeemed token; and

indicating said token is invalid if said current token does not match said last redeemed token and if all tokens in said pool generated after said received token have been examined.

63. (Original) The program storage device of claim 50 wherein said one or more delivery parameters comprises a serial number uniquely identifying said target device.

64. (Original) The program storage device of claim 50 wherein said one or more delivery parameters comprises a master key indicator for use in decrypting an encrypted form of said digital content.

65. (Original) The program storage device of claim 50 wherein said one or more delivery parameters comprises a key derivation process indicator for use in deriving a cryptographic key for decrypting an encrypted form of said digital content.

66. (Original) The program storage device of claim 50 wherein said one or more delivery parameters comprises a cryptographic process indicator that specifies a cryptographic process supported by said target device.

67. (Currently Amended) An apparatus for digital content access control, comprising:

means for receiving, by a content repository, an authenticated digital content request, including one or more delivery parameters, from a user device, said authenticated digital content request based at least in part on a digital content request comprising a request for digital content wherein said authenticated digital content request was generated by a content provisioner in response to said digital content request from said user device;

means for validating, by said content repository, said authenticated digital content request, said validating comprising indicating said authenticated digital content request is valid if said authenticated digital content request is validly associated with said digital content and if said authenticated digital content request authenticates said digital content request;

means for determining, by said content repository, a session key if said authenticated digital content request is valid, said means for determining comprising:

means for determining a target key based at least in part on a target ID, said target ID identifying a target device; and

means for applying a cryptographic process to a first key based at least in part on at least part of said authenticated digital content request together with said target key to create said session key;

means for encrypting, by said content repository, said digital content using said session key; and
means for sending, by said content repository, said encrypted digital content.

68. (Original) The apparatus of claim 67 wherein said means for determining said target key comprises:

means for determining a master key; and

means for applying a cryptographic process to said target ID together with said master key to create said target key.

69. (Original) The apparatus of claim 68 wherein said determining said master key is based at least in part on said one or more delivery parameters.

70. (Currently Amended) The apparatus of claim 67, further comprising means for synchronizing said content repository with a content provisioner if said synchronizing is enabled.

71. (Original) The apparatus of claim 67 wherein said digital content request comprises a Universal Resource Locator (URL); and
said authenticated digital content request comprises a tokenized URL.

72. (Original) The apparatus of claim 71 wherein

said tokenized URL further comprises a token comprising a cryptogram based at least in part on an identifier that describes the location of said digital content; and

said at least part of said authenticated digital content request comprises said token.

73. (Original) The apparatus of claim 72 wherein said first key comprises a token key based at least in part on said token.

74. (Original) The apparatus of claim 72 wherein said token is from a token pool associated with the location of digital content for which access is authorized.

75. (Original) The apparatus of claim 67 wherein said means for validating further comprises:

means for receiving a token;

means for indicating said token is invalid if said token is not found within a token pool associated with said digital content or if said token has been fully redeemed, said token being fully redeemed if the number of token redemptions equals a predetermined amount; and

means for incrementing a token redemption count associated with said token and indicating said token is valid if said token is found within said token pool and said token has not been fully redeemed.

76. (Original) The apparatus of claim 67 wherein said means for validating further comprises:

means for receiving a token;

means for indicating said token is invalid if said token is not associated with an partially redeemed or unredeemed offset within a token offset window, said token offset window comprising one or more offset entries identified by a base number and an offset from said base number, said one or more offset entries

associated with a token in a token pool formed by applying a cryptographic process to the sum of said base number and said offset from said base number, together with a token chain key, said token pool associated with said digital content; and

means for updating the offset entry associated with said token and indicating said received token is valid if said token is associated with a partially redeemed offset or unredeemed offset within said token offset window.

77. (Original) The apparatus of claim 67 wherein said means for validating further comprises:

means for receiving a token;

means for indicating said token is invalid if said token is not found within a token pool associated with said digital content or if said token has been redeemed, said token pool formed from successive applications of a cryptographic one-way function;

means for indicating said token is valid if said token is found within said token pool and said token has not been redeemed; and

means for invalidating tokens in said token chain that were generated after said received token.

78. (Original) The apparatus of claim 67 wherein said means for validating further comprises:

means for receiving a token;

means for indicating said token is invalid if said token is not found within a portion of a token pool comprising unredeemed tokens, said token pool formed from successive applications of a cryptographic one-way function;

means for indicating said token is valid if said token is found within said token pool and said token has not been redeemed; and

means for reordering tokens in said token pool after said indicating said token is valid, said reordering based at least in part on whether the tokens have been redeemed.

79. (Original) The apparatus of claim 67 wherein said means for validating further comprises:

means for receiving a token;

means for initializing a current token to said received token;

means for applying a cryptographic one-way function to said current token to create a result;

means for assigning said result to said current token;

means for repeating said applying until said current token matches a last redeemed token or until all tokens in said pool generated after said received token have been examined;

means for indicating said token is valid if said current token matches said last redeemed token; and

means for indicating said token is invalid if said current token does not match said last redeemed token and if all tokens in said pool generated after said received token have been examined.

80. (Original) The apparatus of claim 67 wherein said one or more delivery parameters comprises a serial number uniquely identifying said target device.

81. (Original) The apparatus of claim 67 wherein said one or more delivery parameters comprises a master key indicator for use in decrypting an encrypted form of said digital content.

82. (Original) The apparatus of claim 67 wherein said one or more delivery parameters comprises a key derivation

process indicator for use in deriving a cryptographic key for decrypting an encrypted form of said digital content.

83. (Original) The apparatus of claim 67 wherein said one or more delivery parameters comprises a cryptographic process indicator that specifies a cryptographic process supported by said target device.

84. (Currently Amended) An apparatus for digital content access control, the apparatus comprising:

a content repository comprising:

a memory for storing said digital content;

and

a processor configured to:

receive an authenticated digital content request including one or more delivery parameters, said authenticated digital content request based at least in part on a digital content request comprising a request for digital content;

validate said authenticated digital content request, said validating comprising indicating said authenticated digital content request is valid if said authenticated digital content request is validly associated with said digital content and if said authenticated digital content request authenticates said digital content request;

determine a session key if said authenticated digital content request is valid, said determining comprising:

determining a target key based at least in part on a target ID, said target ID identifying a target device;
and

applying a cryptographic process to a first key based at least in part on at

least part of said authenticated digital content request together with said target key to create said session key; encrypt said digital content using said session key; and send said encrypted digital content.

85. (Original) The apparatus of claim 84 wherein said apparatus is further configured to determine said target key by:

determining a master key; and
applying a cryptographic process to said target ID together with said master key to create said target key.

86. (Original) The apparatus of claim 85 wherein said apparatus is further configured to determine said master key based at least in part on said one or more delivery parameters.